CLAIMS

1. A quantum key distributing method for a quantum cryptographic system including a communication apparatus on a transmission side that transmits, in a predetermined quantum state, a random number sequence forming a basis of an encryption key to a quantum communication path and a communication apparatus on a reception side that measures photons on the photon communication path, the quantum key distributing method comprising:

a check matrix generating step at which the respective communication apparatuses generate an identical parity check matrix (a matrix with an element "0" or "1");

a cyclic code generating step at which the communication apparatus on the transmission side generates a cyclic code (CRC: Cyclic Redundancy Check) for error detection;

a transmitting and receiving step at which the communication apparatus on the reception side holds reception data with probability information obtained as a result of measuring a light direction with a measuring device capable of correctly identifying the light direction and the communication apparatus on the transmission side holds transmission data (a part of the random number sequence) corresponding to the reception data;

an information notifying step at which the communication apparatus on the transmission side notifies, via a public communication path, the communication apparatus on the reception side of error correction information generated based on the parity check matrix and the transmission data and error detection information generated based on the cyclic code and the transmission data;

a transmission data estimating step at which the

communication apparatus on the reception side estimates the transmission data based on the parity check matrix, the reception data with probability information, the error correction information, and the error detection information; and

an encryption key generating step at which the respective communication apparatuses discard a part of the transmission data according to an amount of information laid open to the public and generate an encryption key using remaining information.

2. The quantum key distributing method according to claim 1, wherein the transmission data estimating step includes:

an initial setting step of setting a prior value corresponding to an element "1" in the parity check matrix as initial setting;

an external value updating step of executing, in row units, processing for updating, according to the error correction information, an external value corresponding to the element "1" in the parity check matrix using a prior value corresponding to another element "1" in an identical row and the probability information;

a prior value updating step of executing, in column units, processing for updating the prior value corresponding to the element "1" in the parity check matrix using an external value after the update corresponding to another element "1" in an identical column;

a temporary estimation step of calculating posterior probability based on the probability information and the prior value after the update and judging a temporary estimated word from the posterior probability (hard decision); and

a transmission data estimating step of performing,

when the temporary estimated word satisfies a predetermined condition established between the temporary estimated word and the parity check matrix, error detection for the temporary word using the error detection information, if there is no error, judging that the temporary estimated word is original transmission data, and repeatedly executing, when the temporary estimated word does not satisfy the predetermined condition, the external value updating step, the prior value updating step, and the temporary estimation step using the value after the update until the condition is satisfied.

3. The quantum key distributing method according to claim 2, wherein, at the transmission data estimating step, the error detection information and estimated error detection information generated using the temporary estimated word are compared, if the error detection information and the estimated error detection information coincide with each other, it is judged that there is no error in the temporary estimated word, and, if the error detection information and the estimated error detection information do not coincide with each other, it is judged that there is an error in the temporary estimated word.

4. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key according to quantum key distribution and transmits, in a predetermined quantum state, a random number sequence forming a basis of the encryption key to a quantum communication path, the communication apparatus comprising:

parity-check-matrix generating means that generates a parity check matrix identical with that of a destination

side apparatus that shares the encryption key;

cyclic code generating means that generates a cyclic code (CRC: Cyclic Redundancy Check) for error detection;

information notifying means that notifies, via a public communication path, the destination side apparatus of error correction information, which is generated based on transmission data (a part of the random number sequence) corresponding to reception data of the destination side apparatus obtained as a result of measuring a light direction with a measuring device capable of correctly identifying the light direction, and the parity check matrix and error detection information generated based on the transmission data and the cyclic code; and

encryption key generating means that discards a part of the transmission data according to an amount of information laid open to the public and generates an encryption key using remaining information.

5. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key according to quantum key distribution and measures photons (a random number sequence forming a basis of the encryption key) on a quantum communication path, the communication apparatus comprising:

parity-check-matrix generating means that generates a parity check matrix (a matrix with an element "0" or "1") identical with that of a destination side apparatus that shares the encryption key;

cyclic code generating step [translator's comment: "step" should be corrected to "means"] that generates a cyclic code (CRC: Cyclic Redundancy Check) for error detection;

transmission data estimating means that estimates

original transmission data based on the parity check matrix, reception data with probability information obtained by measuring a light direction with a measuring device capable of correctly identifying the light direction, and error correction information and error detection information received from a destination side apparatus via a public communication path; and

encryption key generating means that discards a part of the transmission data according to an amount of information laid open to the public and generates an encryption key using remaining information.

6. The communication apparatus according to claim 5, wherein the transmission data estimating means sets a prior value corresponding to an element "1" in the parity check matrix as initial setting, executes, in row units, processing for updating, according to the error correction information, an external value corresponding to the element "1" in the parity check matrix using a prior value corresponding to another element "1" in an identical row and the probability information, executes, in column units, processing for updating the prior value corresponding to the element "1" in the parity check matrix using an external value after the update corresponding to another element "1" in an identical column, calculates posterior probability based on the probability information and the prior value after the update and judges a temporary estimated word from the posterior probability, performs, when the temporary estimated word satisfies a predetermined condition established between the temporary estimated word and the parity check matrix, error detection for the temporary word using the error detection information, if there is no error, judges that the temporary estimated word

is original transmission data, and repeatedly executes, when the temporary estimated word does not satisfy the predetermined condition, the processing in row units, the processing in column units, and the temporary estimated word judgment processing using the value after the update until the condition is satisfied.

7. The communication apparatus according to claim 6, wherein the transmission data estimating means compares the error detection information and estimated error detection information generated using the temporary estimated word, if the error detection information and the estimated error detection information coincide with each other, judges that there is no error in the temporary estimated word, and, if the error detection information and the estimated error detection information do not coincide with each other, judges that there is an error in the temporary estimated word.